Privacy and Data Protection issues affecting EU/US ICT development collaboration

Policy Briefing 1

Author: Maarten Botterman, Jonathan Cave, *GNKS Consult BV – The Netherlands*

ICT Policy, Research and Innovation for a Smart Society

November 2016

www.picasso-project.eu

PICASSO has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement N° 687874.

Thanks

Thanks go out to all people who actively participated in the PICASSO Policy Expert Group meeting on Privacy and Data Protection in Washington DC on 20 May 2016 and the PICASSO Policy Webinar on Privacy and Data Protection on 14 October 2016. Special thanks go out to the PICASSO colleagues from the 5G networks, Big Data and IoT/CPS Expert Groups who contributed from the specific perspective of their expertise.

Disclaimer

PICASSO has been financed with support from the European Commission.

Foreword

On January 1st, 2016, the project PICASSO was launched with two aims: (1) to reinforce EU-US collaboration in ICT research and innovation focusing on pre-competitive research in key enabling technologies related to societal challenges - 5G Networks, Big Data and the Internet of Things/Cyber Physical Systems; and (2) to support EU-US ICT policy dialogue related to these domains with contributions related to e.g. privacy, security, internet governance, interoperability and ethics.

PICASSO is aligned with industrial perspectives and provides a forum for ICT communities. It is built around a group of 24 EU and US specialists, organised into the three technology-oriented ICT Expert Groups and an ICT Policy Expert Group, working closely together to identify policy gaps in or related to the technology domains and to recommend measures to stimulate policy dialogue. This synergy among experts in ICT policies and in the three ICT technology areas is a unique feature of PICASSO.

This policy paper focuses on privacy and data protection policy considerations in the EU and the US that affect and are affected by in particular ICT development collaboration related to 5G Networks, Big Data, and Internet of Things/Cyber Physical Systems. The content reflects the results of desk study and subsequent discussion of the resulting Briefing Paper during a workshop hosted by NIST in Washington DC on 20 May 2016 and a Webinar on 11 October 2016, together with written comments by experts collected via email.

It is the first of 5 thematic Policy Papers and accompanying Webinars scheduled for the coming two years. Future subjects for Policy Papers will be Security; Standardisation; Spectrum; and one yet to be decided – currently "Smart Cities". The intent is to provide a clear overview of the most pressing and/or challenging policy issues that confront technological, business and policy collaborations and to develop valid and practical insights into how they can be addressed from a transatlantic multistakeholder perspective operating in a global context.

Our thanks go out to all those who contributed to our understanding of the issues related to Privacy and Data Protection policies in the EU and the US and of the specific policy issues related to the three PICASSO domains by their active participation in our meetings. We could not have done this without them.

Please feel free to share your thoughts via email to maarten@gnksconsult.com.
Looking forward to engaging with you all,

Best regards

Maarten Botterman
Chairman Policy Expert Group
PICASSO project

Dave Farber
Co-Chair Policy Expert Group
PICASSO project

Executive Summary

One objective of the PICASSO project is to bring forward policy recommendations designed to improve EU/US ICT-orientated research collaborations, specifically in the technological domains associated with 5G networks, Big Data, and IoT/CPS. One of the most contested issue sets across the board concerns personal data protection and the closely-related but distinct issue of privacy. This issue set is not only a matter of deep concern to the private sector and to civil society, but is also an increasingly-fraught bone of contention in the government sphere, where national governments and supranational governance entities tussle over criminal justice, national security and other vital national (e.g. economic) interests. The increasing awareness by individuals of rights to privacy and to personal data protection put this even more directly at the heart of policy discussions and practical developments.

These issues are critical to policy, technology and economic development; the playing field, influences and consequences are global and the US and the EU both have prominent roles and responsibilities to their citizens and to the world. However, their collaboration and cooperation are sometimes hindered by the very different ways in which their law and policy frame both privacy and data protection. However, although US and EU government regulations, enforcement activities and bargaining positions in international agreements differ, there is little evidence that the people, businesses or scientists involved adhere to distinct 'European' or 'US' positions.

This means that both regions' laws and regulations have to be respected and the concerns of non-government stakeholders have adequately to be addressed if ICT developments are to be <1> legally acceptable on both sides of the Atlantic and <2> trusted enough, for now and the years to come, to be adopted – and adapted – for wider use in society.

To avoid legal challenges and crippling uncertainty, it is important for any services offered in Europe that involve the use of data that may be related to persons to be set up to respect the key conditions for dealing with personal data under the General Data Protection Regulation, which will take full effect by May 2018 and for services offered in the US to conform with the essential elements of US data protection rules, especially as related to the specific types of data (e.g. health and financial) that are the subject of dedicated regulations.

PICASSO provided a space for ICT developers and policy analysts from the EU and US to discuss this and related aspects during 2016. For the specific ICT technological areas on which PICASSO focuses on the following conclusions were drawn:

- 5G networks: sensors and tracking will become even more ubiquitous than they are today, as 5G networks will be designed with a focus on data collection and exchange. Therefore, EU/US policy differences do not seem to affect directly the ability of 5G researchers to collaborate on ICT research and innovation;
- Big Data: as a general rule, personal data should not be shared except under data subjects' explicit intent and consent. However, the growing scope and intensity of big data and algorithmic analytics allow data that were never intended to be "personal" to be linked to private individuals. There is a clear need to ensure that big data services remain anchored in a clear framework connecting intent, consent and the uses of data collection and processing in order to ensure their legality and ethical soundness;

- The Internet of Things and Cyber Physical Systems: CPS are not intentionally designed to track individuals. However, many of the devices of which they are composed have this capability, and both the combination of multiple data and the emergent systemic functions of such systems may – actually or apparently – infringe privacy by linking data to data subjects in unexpected or unintended ways. It will be very important to determine which data are, or may become, privacy sensitive, and to determine the best way to define and implement intent and consent conditions. In particular, the IoT is a big data generator (see the arguments above).

This calls for further consideration of taxonomies of data, services and outcomes within each of the three PICASSO domains to identify opportunities and impediments for EU-US ICT research collaboration. It further argues for recognition of the need to build ethical considerations into product innovation, development and deployment; the issues are global and can only be addressed in a multistakeholder way that reinforces transparency in the use of personal data in applications and accountability of actors in the value chain.

Because challenges in the field of privacy and data protection also offer opportunities (for those who find the best ways to address them), legislators should not block "responsible innovation" with disproportionate or unnecessary pre-emptive legislation that may hinder, distort or otherwise limit the benefits of innovation and economic growth. At the same time, industry and the research community should cultivate and demonstrate awareness of people-related issues when developing and deploying new technologies and services and define and adhere to standards of responsibility and self-regulation that come with what ISOC/IETF calls "permissionless innovation" to ensure that society continues to support and to benefit from healthy innovation.

People within the EU and US – and around the world - want and deserve ICT products and services that serve their interests and can be trusted by them, and need ICT products and services to deal with 'wicked' societal challenges. Better EU-US ICT research collaboration can hugely advance this.

Conclusion: in particular with regards to *Big Data* and *IOT/CPS* developments, solutions need to be found to facilitate the development and deployment of needed and desired services, while respecting the (European and US) privacy and data protection frameworks. This will require respecting fundamental privacy and data protection rights by living up to the principles of purpose limitation, data minimisation and explicit consent with all data that could be related to private individuals. In this, beyond the obvious:

- Algorithms – and interacting systems of algorithms – will need to be designed and allowed to operate only "in law abiding ways" – e.g. not combining data in ways that affect the privacy of individuals without an explicit, legitimate and valid justification (such as meaningful and informed consent). This requires a clear understanding of acceptable practice and access to "trusted expertise" (and methods of algorithmic regulation that do not simply rely on code audit) in order to establish this (not widely available today);
- Taxonomy of privacy sensitivity in ICT development – some services and data are more privacy sensitive than others, and some expose limitations and inconsistencies in our understanding and protection of privacy-related rights. Such a taxonomy – and the effort to develop it - would help to improve mutual understanding of these issues and provide clarity to ICT developers on this aspect of the "ethical consequences" assessment;

- Diversity and harmonisation – the EU and the US have different approaches to the legal and regulatory aspects of data protection and privacy, but the technological, market and cultural environments in which these issues play out are not defined by or contained within their separate jurisdictions. There is a need to further clarify the relation between the issues, technological and market development and regulatory structures in order to determine: i) the extent to which the legal framing of these issues can and should be harmonised or aligned; and ii) whether and how existing differences can be a source of useful comparative advantage and informative natural experiments.

Towards the Summer of 2018, we intend to deliver a White Paper on policy issues such as privacy and data protection, security, standardisation and spectrum that are most relevant to technological and commercial development in the PICASSO domains and conversely to identify the aspects of such policies that are most likely to be affected by 5G, Big Data and IOT/CPS development. This PICASSO Policy Paper and the ones that follow will feed in to this White Paper, therefore we invite you to share any comments and suggestions relating this policy paper with the PICASSO Policy Expert Group either in person during one of our meetings (workshops or webinars) or via email to the Chairman of the Policy Expert Group at maarten@gnksconsult.com.

Introduction

One objective of the PICASSO project is to bring forward policy recommendations designed to improve EU/US ICT-orientated collaborations, specifically in the domains associated with 5G networks, Big Data, and IoT/CPS. One of the most contested horizontal issue sets concerns personal data protection and privacy (closely related to each other but not same thing). These issues are not only a matter of concern to the private sector and to civil society, but are also an increasingly-fraught bone of contention in the government sphere, where national governments and supranational governance entities tussle over criminal justice, national security and other vital national interests – and where progress towards a workable common framework has been at best intermittent. The increasing awareness of individuals of the importance of privacy and personal data rights further strengthens their technological, commercial and policy salience.

These domains are neither wholly distinct nor wholly technological; they overlap in the technological, economic/commercial, business and societal planes. Each of these planes creates a shared perspective on the common problems and thereby serves as a platform for intra-plane and inter-plane multistakeholder interaction. Problems, issues or challenges may have their causes in one (set of) planes, their effects in another and their solutions in a third. Therefore, the interactions (here called 'collaborations') in fact combine collaboration with competition. Concretely, privacy issues can be resolved by technological, economic and policy measures or by the evolution of societal norms adapted to the modern technological and economic dimensions of privacy. For instance, as the possibilities for infringing privacy and the value of doing so change, the norms defining acceptable behaviour and the sanctions for violating them also change. Whether EU/US collaboration leads to societal, technological, economic, or policy/regulatory 'solutions' will depend on a competitive struggle (across markets, labs and legislatures) as much as it does on a cooperative, neutral and civilised discussion. This mix of modes (cooperation, competition and conflict) can clearly be seen in e.g. TTIP and Privacy Shield.

Although PICASSO will not be able fully to address all stakeholder concerns, it aims to explore how US/EU collaboration in ICT can best be served, taking into account the differences in approach towards privacy and data protection in the US and in Europe, respecting the law and citizens' expectations and preserving the widest possible scope for innovation and deployment. In this policy paper, the origin and specific aspects of applicable legislation in the European Union and US are explored and compared.

EU and US Policy Frameworks

In addition to being important topics in their own right, privacy and data protection issues complicate trade negotiations, freedom of information rules, digital rights, intellectual property protection and financial regulation. With particular reference to the transatlantic dimension and the specific PICASSO domains of 5G networks, Big Data, and IoT/CPS, they feature in the evolving arrangements over corporations' personal data collection, storage, processing and access (contrasting the EU-US Privacy Shield, which tends to restrain businesses, with those provisions in TTIP, TPP and especially TSIA that effectively protect corporations from government restraint).

Beyond this direct consideration of transatlantic data flows are indirect tensions arising from divergent legislative and legal developments. US moves to limit government powers to compel businesses to

provide access to personal data (especially bulk phone records) e.g. in the US Freedom Act can be contrasted with the enhanced powers over acquisition of communications data, interception of communications, bulk personal datasets and equipment interference on the other hand, such as those detailed in the UK's recent Investigatory Powers Bill and its accompanying Code of Practice[1]. These raise a range of thorny questions, including a consideration of whether Europe's data protection apparatus reflects a legitimate regional ethical stance (privacy as a fundamental rather than an economic right) or could be considered a protectionist barrier to commerce and a hindrance to economic growth[2].

Differences in legal status of privacy

The context for these developments – and a major potential stumbling block or opportunity – is provided by the complex and very different framing and legal status of privacy both between the US and Europe and within Europe. The EU tends (with some Member State and data type exceptions) to view data privacy as a *fundamental right* independent of founding documents such as the TFEU)[3]. It is important to note that all Member States of the European Union are part of a larger regional intergovernmental organisation, the Council of Europe, which has its own legislation on privacy and data protection: the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108). This Convention is the legal articulation of the protection of personal data and privacy enshrined in article 8 of the European Convention on Human Rights. This open convention is – at this point – the sole international legally binding instrument dealing with data protection and privacy; it is seen by other international organisations (such as UN and OECD) and nations to represent the quintessence of the legal provisions in the matter. The US tends to move towards an *economic* right interpretation deriving explicitly from a Constitutional base. The EU applies privacy protections to *broad classes* of data collection and handling (in the General Privacy Regulation which will come into force in 2018), while the US protects only *specific types* of data (e.g. health-related and financial, see below). The EU has only recently framed a *general Right of Erasure*[4] - its exercise is a responsibility of data subjects and liability for complying remains with data controllers. By contrast, the US *mandates erasure of specific data*[5].

The EU focuses on protecting citizens against *data privacy* invasion by *private sector actors*, while the US Constitution's Fourth Amendment protects citizens against "unreasonable search and seizure" *by government* and has (through Supreme Court decisions) used the Due Process clause of the Fourth Amendment to recognise 'unenumerated' or shadow privacy rights that go well *beyond mere data*

[1] For the Bill and Codes of practice, see https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/473770/Draft_Investigatory_Powers_Bill.pdf and https://www.gov.uk/government/publications/investigatory-powers-bill-codes-of-practice.
[2] As Carl Bildt of the Global Commission on Internet Governance put it: "Barriers against the free flow of data are, in effect, barriers against trade." Cf. http://www.ft.com/cms/s/0/5d626a4e-f182-11e4-88b0-00144feab7de.html#axzz3fad5AuLJ.
[3] This is explicitly reflected in the recent European Court of Justice ruling invalidating the Safe Harbour Agreement on the grounds of incompatibility with "fundamental rights and freedoms, notably the right to privacy" (cf. http://static.ow.ly/docs/schrems_3OHQ.pdf.
[4] See Articles 17 and 19 of the General Data Protection Regulation – note that Article 17(2) requires data controllers to notify third-party processors that an erasure request has been made, and makes them liable. See text at: http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2014-0212&language=EN.
[5] E.g. health data - HIPAA (Health Insurance Portability and Accountability Act) and financial data - FACTA (The Fair and Accurate Credit Transactions Act of 2003); GLB (Gramm-Leach Bliley); Sarbanes-Oxley Act (SOx); and Payment Card Industry Data Security Standards (PCI DSS).

protection. Another difference is the largely negative cast of US rights, which *prohibit* government from taking certain actions against its citizens compared with the EU framework's addition of 'affirmative' provisions *requiring government actively to protect rights* against infringements by other actors. This approach in Europe is more provided by the European Court of Human Rights which delivers judgements on issues where individual human rights are infringed by governments.

The net result of these differences has led to a tendency for US negotiators to treat privacy primarily as a trade issue, while their EU counterparts see the issue as necessarily going well beyond commercial or economic considerations and mechanisms. Even mutual recognition does not necessarily provide a starting point for agreement, as 'mutuality' is so hard to define.

There are opportunities as well. Different approaches can reveal latent preferences such as the appetite of US consumers for anonymous profiling tools developed to protect data subjects while making their data suitable for economic use. The use of different approaches despite roughly similar technologies, services and business models creates an ideal natural experiment to help separate essential from inertial aspects of privacy and to point the way to suitable 'bridging' frameworks. Also recognising that a "privacy sensitivity taxonomy" would help to identify those areas where the differences in approach do not affect the ability for EU-US ICT collaboration, and creating such a taxonomy, could potentially be hugely beneficial.

More and more emphasis has been put by citizens/consumers on privacy in an increasing digital world. Awareness is raising, although few people today are well informed about the real issues, and anecdotal research demonstrates time and time again that the "costs of privacy" vary greatly depending what is on offer.

As said in the introduction: the basis for legislative protection of data and privacy is different in the US and In Europe: so is the legislative approach. At EU the basis can be found in the Lisbon Treaty and the Charter of Fundamental Rights and on the U.S. side in the U.S. Constitution.

EU legislation has been moving recently from its original guidance by the Data Protection Directive of 1995 (further: DPD) towards the General Data Protection Regulation which will be fully in force by May 2018 (further: GDPR), thus to allow European Member States to adjust their national legislation that was put in place pursuant the DPD towards the now European level legislation. US legislation regarding to data protection is merely sectoral and subject to individual Court's Decisions (Case Law). Both the EU and US developing frameworks are described below.

Europe: the General Data Protection Regulation

When the original Data Protection Directive was developed and agreed in 1995, the Internet was by far not as important as today, and nobody had even mentioned the term "Internet of Things" yet. A review of the 1995 Directive in 2009, sponsored by the UK Data Privacy Authority, already noted that new developments like IoT, data mashups and data virtualisation are new challenges that had to be met[6]. The reform that led to the new General Data Protection Regulation (further: GDPR) has been under way since 2011 and culminated in a Proposal to Council and Parliament by the European Commission on 25 January 2012. This proposal was approved by the European Parliament in March

[6] Neil Robinson, Hans Graux, Maarten Botterman & Lorenzo Valeri. Review of the EU Data Protection Directive, prepared for the Information Commissioner's Office, TR-710-ICO. Cambridge, May 2009

2014, and has now been finalised and ratified by Parliament and Council to come into force in May 2018.

With this, it should be noted that the work has not been completed. When this law was set up in outline in 2011, "Big Data" was not yet an issue widely recognised, in that year new in the Gartner Emerging Technologies Hype Cycle. Today, we know that big data, and big data analytics, fundamentally challenge the concept of "personal data" as through big data analytics data that in isolation do not relate to persons often can be related to persons when combined with other data. Published in 2014, the Opinion from WP29[7] on IoT recognised the value of IoT, as well as the potential intrusions it can generate to privacy. Future developments in increasing abilities and new ways of using technologies and data will continue to be considered in the light of the current Legislative framework. In this spirit the Consultative Committee of Convention 108 has started to draft a guide on big data and is about to finalise it (it is due to get adopted by the end of 2016) which will be the first of its kind and which could serve as point of orientation for different actors in the future.

US: Case Law based on the Constitution

The US has no single data protection law comparable to the EU's Data Protection Regulation. In the US privacy legislation has developed on an ad hoc basis when required by certain sectors and circumstances. Fundamental within the US is "The Fourteenth Amendment (Amendment XIV)" which was adopted in the United States Constitution on July 9, 1868[8]. The Amendment addresses citizenship rights and equal protection of the laws, and was proposed in response to issues related to former slaves following the American Civil War. The first section of The Fourteenth Amendment is one of the most litigated parts of the Constitution and has been used as the basis or a number of landmark decisions, e.g. such as Roe vs. Wade (1973) regarding abortion, Bush vs. Gore (2000) regarding the 2000 presidential election, and Obergefell vs. Hodges (2015) regarding same-sex marriage. Critically the amendment limits the actions of all state and local officials, including those acting on behalf of officials.

The right to privacy or the "right to be left alone" is a key area within the US. While not explicitly stated in the U.S. Constitution, some of the amendments provide a degree of protection towards privacy. Privacy is most often protected by statutory law in the US. For example the Health Information Portability and Accountability Act (HIPAA) protects a person's health information, and the Federal Trade Commission (FTC) enforces the right to privacy in various privacy policies and privacy statements.

There is a challenge, however, when there is a need to balance privacy against the needs of public safety and improving the quality of life, in some ways comparable to legislation related to traffic safety such as seat-belt laws and motorcycle helmet requirements. Most Americans accept that government surveillance and collecting of personal information is necessary. The right to privacy often relates to the right to personal autonomy where an individual has the right to choose whether or not to engage

[7] The Article 29 Data Protection Working Party was set up under the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. It has advisory status and acts independently.

[8] Legal analysis from PICASSO Deliverable 1.3 *Panorama of ICT landscape in EU and US: ICT, Policies, regulations, programmes and networks in the EU and US*. Authors: Haydn Thompson and Daniela Ramos-Hernandez, THHINK – UK

in certain acts or have certain experiences. Several amendments to the U.S. Constitution have been used in varying degrees of success in determining a right to personal autonomy:

- The First Amendment protects the privacy of beliefs
- The Third Amendment protects the privacy of the home against the use of it for housing soldiers
- The Fourth Amendment protects privacy against unreasonable searches
- The Fifth Amendment protects against self-incrimination, which in turn protects the privacy of personal information
- The Ninth Amendment says that the "*enumeration in the Constitution of certain rights shall not be construed to deny or disparage other rights retained by the people*." This has been interpreted as justification for broadly reading the Bill of Rights to protect privacy in ways not specifically provided in the first eight amendments.
- The 14th Amendment includes a Due Process Clause which states: "*No state shall make or enforce any law which shall abridge the privileges or immunities of citizens of the United States; nor shall any state deprive any person of life, liberty, or property, without due process of law; nor deny to any person within its jurisdiction the equal protection of the laws.*"

The protections have been narrowly defined and are usually interpreted as only applying to family, marriage, motherhood, procreation and child rearing. The controversial *Roe v. Wade* case in 1972 case 142 established the right to privacy as fundamental, and required that any governmental infringement of that right had to be justified by a compelling state interest.

In the US a person has the right to determine what sort of information about them is collected and also how that information is to be used. In the marketplace this is enforced by laws intended to prevent deceptive practices and unfair competition. The Privacy Act of 1974 prevents unauthorised disclosure of personal information held by the federal government. A person has the right to review their own personal information, ask for corrections and be informed of any disclosures. This has also been imposed upon financial institutions in the Financial Monetization Act (1999) which requires financial institutions to provide their customers with an explanation of what kind of information is being collected and how it is being used. Safeguards are also required to protect customer information, e.g. the Fair Credit Reporting Act, protects personal financial information collected by credit reporting agencies. The act puts limits on who can access the information and requires agencies to have simple processes by which consumers can get their information, review it and make corrections.

Online privacy is also important in the US and Internet users can protect their privacy by taking actions that prevent the collection of information, for instance to not allow tracking cookies. Browsers and social media platforms, e.g. Facebook and Twitter, allow user selected privacy settings, from sharing everything to only sharing with friends. At a minimum level this can be only a name, gender and profile picture and increasingly citizens are aware that it is necessary to protect personally identifiable information to prevent identity theft.

Also within the US the Children's Online Privacy Protection Act (COPPA) enforces a parent's right to control what information websites collect about their children. In particular websites that target children younger than 13 or knowingly collect information from children must post information on

their privacy policies and also get parental consent before collecting information from children. Parents can thus decide how such information can be collected.

As well as a right to privacy there is also a right to publicity. Here there is a right to control the use of his or her identity for commercial promotion. Unauthorised use of someone's name or likeness is recognised as an invasion of privacy. This is classed into 4 areas: intrusion, appropriation of name or likeness, unreasonable publicity and false light. For instance, if a company falsely uses a person's photo in an advert claiming that the person endorses a product, the person can file a lawsuit claiming misappropriation.

The Supreme Court in the US approaches the right to privacy and personal autonomy on a case-by-case basis. Notably public opinion is constantly changing regarding relationships and activities. The boundaries of personal privacy are also changing due to social media and a move towards "sharing." As a consequence, the definition of the "right to privacy" is constantly subject to changing interpretation.

The EU/US agreement Privacy Shield

The international Safe Harbour Privacy Principles enabled some US companies to comply with privacy laws protecting European Union and Swiss citizens by self-certifying that they adhere to the 7 principles underlying the European Data Protection Directive without further need for a formal certification process as would have been required otherwise by the European Data Protection Directive related national legislations.

In 2015, a Court Ruling by the European Court of Justice in the case of Maximillian Schrems versus the Irish data protection commissioner regarding the right of Facebook to transfer data to servers located in the US under the Safe Harbour scheme declared the Safe Harbour Decision invalid. Reason given was that the protections under the Safe Harbour scheme provided by the US Authorities had proven to be inadequate, in particular because "*the scheme is applicable solely to the United States undertakings which adhere to it, and United States public authorities are not themselves subject to it. Furthermore, national security, public interest and law enforcement requirements of the United States prevail over the Safe Harbour scheme, so that United States undertakings are bound to disregard, without limitation, the protective rules laid down by that scheme where they conflict with such requirements*" and because for non-US citizens there is no opportunity to redress: "*legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data, compromises the essence of the fundamental right to effective judicial protection*".[9]

IoT providers and Big Data companies such as the globally popular "Nest" smart meters and smoke detectors, owned by Google, continued to refer to "Safe Harbour Agreement" protection of personal data as there was no immediate alternative[10]. The measures currently proposed by the European Commission to replace "Safe Harbour", known as "Privacy Shield"[11], were approved by the EU Member

[9] ECJ ruling in case C-362/14 Maximillian Schrems vs Data Protection Commissioner, 6 October 2015, see http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf

[10] https://nest.com/legal/privacy-statement-for-nest-products-and-services/

[11] The EU-U.S. Privacy Shield imposes stronger obligations on U.S. companies to protect Europeans' personal data and requires the U.S. to monitor and enforce more robustly, and cooperate more with European Data Protection Authorities. It also includes written commitments and assurance regarding access to data by public authorities.

States representatives (Article 31 Committee) on 8 July 2016, following which the European Commission adopted the framework on 12 July 2016 and it went into effect the same day. It should also be noted that this new agreement has not been tested in Court, yet, and until this is done and ruled to be a "valid agreement" uncertainty about this new protection remains.

ICT development impacts

Technology impacts go two ways: legislator frameworks influence how technologies are developed, and technology developments, at times disruptive of nature, can either support or challenge legislation and/or legislator frameworks. The three technology subjects that are in the focus of PICASSO affect and are affected by the legal frameworks on both sides of the Atlantic.

This is already widely recognised, and businesses are looking for guidance. Continuous (and increasingly rapid) changes in technology and society linked to the spread of ICTs complicate framing the issues, and at the same time highlights the opportunities that EU-US ICT collaboration can bring. ICT has become global as ICT products and services are potentially used anywhere in the world, and increasingly with localisation of data, software and hardware at places independent from the geographic location of the user. Examples of challenges that this brings include:

- *Increase of data capture and sharing across networks independent of geographic borders*, even more so when growing towards an ubiquitous 5G network supported environment;
- *Difficulty of separating private data* of multiple individuals from non-private data following Big Data developments and across national borders in order to establish the limits of commercial exploitation and government access;
- Extent and nature of privacy threats and protections connected with the Internet of Things, even more so as data, IoT networks and "connected Things" themselves cross borders;
- Status of data storage and processing facilities used in cloud computing;
- Commercial and legal implications of data protection rules for (big or small) data analytics and of encryption in communications and storage.

Below the specific aspects are considered relating to the three PICASSO ICT collaboration areas: 5G Networks; Big Data; and Internet of Things/Cyber Physical Systems.

5G networks

In our move towards a hyper-connected society, 5G networks are likely to play a major role. Building on the 4G achievements 5G networks will also facilitate massive amounts of sensors, both mobile and fixed, using relatively little energy, and ultra-reliable communications that can serve as (very) remote controls. Following full implementation of 5G the world will be ready to further tag, track and trace any object that is substantial enough for you to want to know where it is – from bikes to computers to basically any gadgets over 50 USD/EUR in purchase. Through the ability to be connected everywhere, all the time, including location tagging, additional masses of data become available that may be related to natural persons – if not directly than through the use of other data and algorithms or artificial intelligence.

Danger is that through this it will become possible to track and trace and relate to natural persons which would enable privacy infringements that go well beyond anything we have seen today. This is

already possible today, yet connectivity networks are still relatively patchy and it is costly to do. With networks becoming more ubiquitous and costs of additional tracking and tracing going down dramatically, regulation will be needed to constrain businesses (and governments?) from fully going there. Self-regulation, or regulation via international and national law? Certainly, a first step will be awareness raising among citizens, consumers and policy makers and the potential effects, and a multistakeholder dialogue to result in how to deal with this. Core in this is access and use of data, either by persons or machines/algorithms.

An opportunity for EU/US collaboration is development of systems in such a way that location and exchange of data are transparent to those that are in the system, and that alternatives are available. In addition, a "code of ethics" that is applicable for both EU and US, or indeed at global level could be developed that determine the limits of data gathering and combination, balancing societal and commercial interests with the privacy and data protection principles that are considered a fundamental right in Europe. A particular issue of attention are algorithms that will need to be set up to act "ethical" (respecting fundamental rights).

Big Data

Big Data is a subject of interest to many, and companies as well as governments around the world are looking into the opportunities offered by Big Data, including data generation, collection, and analytics. With the connection between data through communication networks it has become possible to access and relate masses of data, potentially to fine detail relating to private individuals. The ability to combine masses of data comes not only with this threat, but also with the promise of new ways to be able to effectively deal with societal challenges, and business challenges.

Challenges will be to create new services within the boundaries of the Law that currently (in Europe) disallow use of personal data for other purposes than those that were indicated when collecting them. In particular, this limitation would keep developers from the EU a global market where others (for as far as they are *not* using data on European citizens) have much more room for manoeuvring.

Opportunities will be in creating ecosystems that are trusted and complying with data protection legislation, providing services private individuals want and are consenting to. By creating such services that both comply with US and EU law a product is developed that can have global impact.

Uncertainty about acceptable arrangements under the developing privacy and data protection regulatory frameworks affects the willingness of investors to invest in projects that may be seen as "privacy sensitive" and subject to data protection rules (and fines). According to the European Data Protection Supervisor (EDPS) Peter Hustinx[12]: "If Big Data operators want to be successful, they should … invest in good privacy and data protection, preferably at the design stages of their projects". With this, he recognises the important of "soft law" at this point[13]. Investing in good privacy and data protection should be core in the innovation, development and deployment of IoT, and probably a pre-condition for European (co-)sponsored research. A way forward could include the habit/obligation of a Privacy Impact Assessment in every stage of design of new IoT products and services.

[12] Peter Hustinx according to Mark Say in the article "Big data needs big guidance" in FT, December 29, 2014. Retrieved http://www.ft.com/cms/s/0/fab4bae8-7f88-11e4-86ee-00144feabdc0.html#axzz3O8I1GAvc on 2015.01.07

[13] See also: Europe's policy options for a dynamic and trustworthy development of the Internet of Things, RAND, June 2013

In the Opinion on Digital Ethics[14] published by his successor EDPS Giovanni Butarelli refers to Article 1 of the EU Charter of Fundamental Rights: 'Human dignity is inviolable. It must be respected and protected.' From that position, he further explains that: "In today's digital environment, adherence to the law is not enough; we have to consider the ethical dimension of data processing." It is in line with this that projects funded by the European Commission are looking very carefully at the issue of privacy protection and the idea of limiting the amount of information available to each entity. In general, the key issue to take into account while discussing privacy has to do with the integration of information from different sources. While a single stream of data might not contain enough information to invade the privacy of the user, it is recognised that the correlation and concurrence of information at an entity can lead to privacy considerations that were unthinkable when only looking at the individual sources.

While the user is ultimately responsible for the data it allows to escape in the open, a modern individual that works and lives with current technologies cannot keep up with the types and amount of information being "leaked" by applications and websites. It is, therefore, for an individual virtually impossible to design privacy policies that are permissive enough to allow for services to work, while at the same time, restrictive enough that the privacy of the user is not compromised. Any specific harm or adverse consequence is the result of data, or their analytical product, passing through the control of three distinguishable classes of actor in the value chain[15]:

1. Data collectors, who may collect data from clearly private realms, from ambiguous situations, or data from the "public square," where privacy-sensitive data may be latent and initially unrecognizable;

2. Data analysers, who may aggregate data from many sources, and they may share data with other analysers creating uses by bringing together algorithms and data sets in a large-scale computational environment, which may lead to individuals being profiled by data fusion or statistical inference;

3. Users of analysed data generally have a commercial relationship with analysers; creating desirable economic and social outcomes, potentially producing actual adverse consequences or harms, when such occur.

From the legal perspective, it is necessary to map these actors to the data subject, data processor and data controller roles whose responsibilities are defined in applicable legislation. In particular, it is important to develop and promulgate guidelines that clarify the existing rules as they apply to application and algorithm developers and others, and to appropriately distinguish between data-enabled applications and services that create value through the personalised use of data and those that make statistical or aggregate use of data assemblages. For instance, while it is possible to identify (and therefore unjustly to target) individuals by 'recombinant' data processing, it is not necessary to make such identification in order to identify and make use of correlations among different variables applying to individuals – for example through pseudonymisation. The boundaries of identifiability, the characteristics of data assemblages and responsibilities of those who contribute to the design and implementation of automated means of data analysis are among the areas that could be clarified in this way. This would prevent unnecessary inhibition or distortion of data-enhanced services and minimise e.g. transatlantic distortions without requiring legal changes.

[14] Opinion 4/2015, Towards a new digital ethics: Data, dignity and technology, EDPS, 11 September 2015
[15] Executive Office of the [US] President PACT report: Big Data: Seizing Opportunities, Preserving Values (May 2014)

As the complexity increases through technology, we will depend on technology to deal with it. It is crucial that automated and self-configuring solutions are offered that analyse the type and amount of information given away for a specific user and configure the appropriate number of policies to ensure that the level of security and privacy desired by the user is kept untouched. For this, new innovative solutions are needed as the main challenge seems to be the adequate and consistent interaction between data controller and data subject during the whole process of the increasingly fast data processing. This goes beyond mere regulatory actions and require robust and flexible technology solutions that work under very different conditions, and that are backed by legislation to ensure that abuse of technologies or data is subject to redress and legal action.

Internet of Things/Cyber Physical Systems

Within PICASSO the focus of the IoT activities is specifically on large-scale systems, and industrial and closed-loop systems that connect to physical actuators (or: Cyber Physical Systems: CPS) – including safety critical applications. Most of these will be business-to-business and overall less relevance to private individuals than the IoT domain at large. It is noted that the result of compromising data integrity may go well beyond privacy infringements – it may go at cost of public safety and security, and environmental safety.

A specific challenge in IoT/CPS environments is that data ownership and control may pass through multiple actors, and that information that could relate to private individuals may also be relevant to keep systems safe and secure. In EU/US collaboration we see that limitations in this are more stringent under European legislation (which includes privacy as a fundamental right) than under US legislation.

The opportunity is similar to the Big Data opportunity: by creating IoT/CPS ecosystems that are trusted and complying with data protection legislation, providing services private individuals want and are consenting to. By creating services that both comply with US and EU law products are developed that can have global impact.

Conclusions

A framework for ICT collaboration needs fully to reflect our shared democratic and individual rights-based values, expressed globally in Universal Declaration of Human Rights whereas in Europe in the European Convention on Human Rights, while on the EU side by the Lisbon Treaty and the Charter of Fundamental Rights and on the U.S. side by the U.S. Constitution. They need to reflect the differences that enrich our interaction.

- Privacy and effective exploitation of data can turn out to be opposite sides of the same invaluable coin. Participants agreed that it would be important for industry to explicitly consider the human element and the right of choice from the outset when developing industrial solutions;
- The awareness of policy makers, citizens, consumers and the commercial world of what is technologically possible, economically advantageous, socially acceptable, politically viable, legally allowed and ethical could usefully be raised. It was agreed that those with important decisions to make and those most exposed to the consequences too often have only limited insight into what is happening on the ground.

Solutions need to be found to allow services needed/wanted to get deployed, while respecting the (European and US) privacy and data protection frameworks. Challenges for cooperation on any developments that involve personal data are in the core related to the fact that personal data privacy is considered a fundamental right within the EU, whereas personal data are considered an economic right within the US legal context. In order to avoid legal challenges within the EU it is important for any services –public and private alike- that involve the use of data that may be related to persons to be set up to respect the key conditions for dealing with personal data under the General Data Protection Regulation that will be into full force in May 2018.

Considering this, the following aspects relate specifically to the three PICASSO domains with Privacy and Data protection policies:

- 5G networks: sensors and tracking will become even more ubiquitous than it is today, as networks will be designed with a focus on data collection and exchange. As such, EU/US policies do not seem to directly affect the ability to collaborate in 5G networks ICT research and innovation.
- Big Data: challenges go two ways: <1> personal data may not be shared unless it is set up to be shared by explicit intent and consent; <2> through use of algorithms and big data, data could become related to private individuals that were never intended to be "personal". Here, a clear link to intent/consent will need to be respected in order to ensure big data services to operate in a legal way.
- IoT and Cyber Physical Systems: CPS are not designed to sense/track individuals, but through their operation, individuals may be linked to specific data. It will be very important to determine which data are privacy sensitive and how their collection and processing relate to the intent of the processor and meaningful consent of data subjects – the IoT is a big data generator, and the considerations mentioned above apply.

Particular attention will need to be given to the use of algorithms that allow combining masses of data from different sources and relate those to private individuals, whereas much of these data was never collected for that purpose, nor have explicit user consent for this purpose. There is an increasing awareness of the need to insist that these are build up "in a law abiding way" – i.e. not combining data in ways that affect the privacy of individuals and to develop ways forward that ensure this as much as possible. A second point is the recognition that some services are more privacy sensitive than others – a taxonomy related to new ICT services with regards to this would help create more clarity.

The only way to ensure EU-US collaboration in ICT helps this world evolving in a direction people want through is by recognising that ICT truly has a global impact and affects people, in whatever way, shape or form and thus should be transparent in its use, both in what it does and who is responsible for what in values chains that are facilitated by ICTs. To understand how this can look like, there is a need for a global, fundamental discussion on privacy and the impact of new technologies, as ICT developments in a networked world are global, by definition. This global debate needs to build on the discussion already taking place and to take place in societies around the world, in which the need for balance between private and public interests are weighted and discussed. Answers will not be the same for each society, as there are differences in cultural values and legal frameworks. The debate needs to involve policy makers, businesses, technology developers and citizens around the world as technologies such as those discussed within the PICASSO project rapidly spread and become a more fundamental element of the fabric of our societies every day. The Internet Governance Forum is one

of the global platforms that can support such a debate which will need to take place in a multistakeholder fashion, requiring industry self-regulation and a multilateral government underpinning.

Recognising that the challenges in the field of privacy and data protection also offers opportunities (for those who find the best ways to address them) it is up to the legislators to ensure "responsible innovation" is possible thus not stifling innovation and economic growth where that is not necessary. At the same time, there is a challenge to industry and research to demonstrate awareness of people related issues that are to be considered when developing and deploying new technologies and services – and to ensure that society continue to support innovation above stricter legislative protection.

People within the EU and US want ICT products and services that serve them and are trusted by them, and need ICT products and services for being able to deal with a number of societal challenges and individual preferences. Better EU-US ICT collaboration can hugely advance this.

Operational conclusion, in particular with regards to *Big Data* and *IoT/CPS* developments, are that solutions need to be found to allow services that are needed/wanted can get deployed, while respecting the (European and US) privacy and data protection frameworks. This will require respecting the EU fundamental right on Privacy by living up to the principles of purpose limitation, data minimisation and explicit consent with all data that could be related to private individuals. In this, up and beyond the obvious:

- In the future, algorithms will need to be build up "in a law abiding way" – i.e. not combining data in ways that affect the privacy of individuals. This requires a clear understanding of what is acceptable practice and access to "trusted expertise" in order to establish this (not widely available today);
- Need for a taxonomy on privacy sensitivity in ICT development, as some services are more privacy sensitive than others (this would help to grow understanding on these issues, and help shape clarity to ICT developers on this aspect which could be considered part of the "ethical consequences" assessment.
- Diversity and harmonisation – the EU and the US have different approaches to the legal and regulatory aspects of data protection and privacy, but the technological, market and cultural environments in which these issues play out are not defined by or contained within their separate jurisdictions. There is a need to further clarify the relation between the issues, technological and market development and regulatory structures in order to determine: i) the extent to which the legal framing of these issues can and should be harmonised or aligned; and ii) whether and how existing differences can be a source of useful comparative advantage and informative natural experiments.

Towards the Summer of 2018, we intend to deliver a White Paper on policy issues such as privacy and data protection, security, standardisation and spectrum that are most relevant to technological and commercial development in the PICASSO domains and conversely to identify the aspects of such policies that are most likely to be affected by 5G, Big Data and IOT/CPS development. This PICASSO Policy Paper and the ones that follow will feed in to this White Paper, therefore we invite you to share any comments and suggestions relating this policy paper with the PICASSO Policy Expert Group either in person during one of our meetings (workshops or webinars) or via email to the Chairman of the Policy Expert Group at maarten@gnksconsult.com.